

PENERAPAN VERNAM CIPHER DAN ROT13 PADA SISTEM KEAMANAN SMS (*Short Message Services*)

¹ *Firlian Okto Hari Pratama (1110651102)*

² *Lutfi Ali Muharom, S.Si* ³ *Hardian Oktavianto, S.Si*

Program Studi Teknik Informatika Fakultas Teknik

Universitas Muhammadiyah Jember

Email : firlianpratama04@gmail.com

ABSTRAK

Algoritma *One Time Pad* (OTP) yang merupakan algoritma yang relatif gampang untuk dipelajari dan sudah dinyatakan oleh para ahli kriptografi sebagai “*perfect encryption algorithm*”. Sedangkan *ROT13* adalah substitusi kode dengan melakukan pergeseran sebanyak $k=13$. Digabungkan dengan teknik algoritma *encoding* karakter *base64*. *Base64* adalah sebuah *encoding* karakter yang mewakili data biner dalam format string ASCII dengan menerjemahkannya ke dalam representasi 64. Dengan menggunakan Algoritma *Vernam Cipher* dan *ROT13* sebagai pengamanan teks SMS (*Short Message Services*) yang diimplementasikan pada Sistem Pengamanan SMS didapat hasil bahwa Sistem ini dapat melakukan enkripsi pesan sms dengan baik untuk melakukan pengamanan pesan yang dikirim ke nomor lain. Akan tetapi Sistem Enkripsi Pesan SMS ini tidak dapat mendeskripsikan pesan yang berjumlah 160 karakter ke atas yang dikarenakan pada proses enkripsi pesan akan menjadi lebih banyak dari *plaintexts* pesan sehingga proses pengiriman pesan akan dipotong per 160 karakter (panjang pesan untuk SMS maksimal 160 karakter) sehingga terjadi kegagalan proses karena tidak lengkap serta sistem ini sangat berpengaruh pada *random key*, jika *random key* yang dihasilkan dapat mendekode maupun mengmodulus secara sempurna maka pesan dapat dideskripsi secara baik dan sebaliknya.

Kata Kunci : SMS, Random, Key, ROT13, OTP.

APPLICATION VERNAM CIPHER AND SECURITY SYSTEM ROT13 SMS (Short Message Services)

¹ *Firlian Okto Hari Pratama (1110651102)*

² *Lutfi Ali Muharom, S.Si* ³ *Hardian Oktavianto, S.Si*

Informatic Engineering Program, Engineering Program

Jember Muhammadiyah University

Email : firlianpratama04@gmail.com

ABSTRACT

Algorithm One Time Pad (OTP) algorithm which is relatively easy to learn and has been declared by experts cryptography as "the perfect encryption algorithm". While ROT13 is a substitution code by shifting as much as $k = 13$. Combined with engineering algorithms base64 encoding characters. Base64 is an encoding characters that represent binary data in ASCII string format to translate into representation 64. By using the Vernam Cipher Algorithm ROT13 as pengamankan text and SMS (Short Message Services) which was implemented in SMS Security Systems obtained the results that this system can perform encryption sms message well to secure messages sent to another number. However, this SMS Message Encryption System can not describe the message that amounted to 160 characters upwards due to the process of message encryption will become more of a plaintext message so that the message delivery process will be deducted per 160 characters (long SMS messages to a maximum of 160 characters) that occurred failure of due process is not complete and the system is very influential on the random key, if randomly generated key can decode and perfectly mengmodulus then the message can be described as good and vice versa.

Keywords: *SMS, Random, Key, ROT13, OTP.*